Federal Information Security Management Act and Defense Health Program System Inventory Reporting Tool

2008 Data Protection Seminar

TMA Privacy Office

FISMA and DHP-SIRT

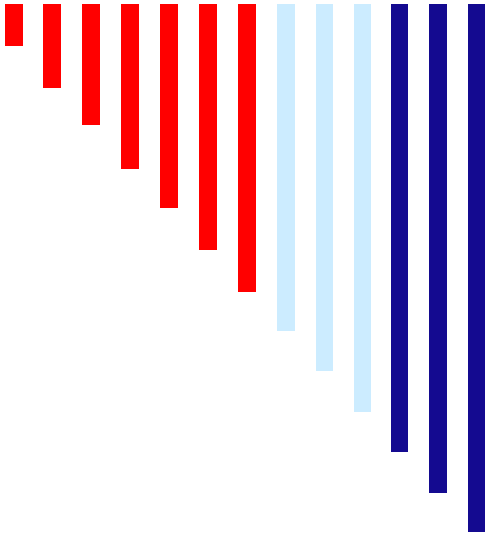
Purpose

- Provide an overview of the Federal Information Security Management Act (FISMA), the Defense Health Program System Inventory Reporting Tool (DHP-SIRT), and the importance in privacy reporting

FISMA and DHP-SIRT

Objectives

- This presentation will:
  - Demonstrate the purpose of FISMA
  - Show how privacy reporting is related to FISMA
  - Identify the new Privacy requirements for FISMA
  - Describe DHP-SIRT and its impact
  - Identify the new data fields associated with Privacy in DHP-SIRT



FISMA

FISMA and DHP-SIRT

The Establishment of FISMA

- Report required by the E-government Act of 2002, Title III
- Report on the security and privacy of sensitive information in Federal computer systems on:
  - System inventories
  - Testing and evaluation
  - Security controls
  - Privacy controls

FISMA and DHP-SIRT

FISMA Scorecard

FEDERAL COMPUTER SECURITY REPORT CARD			May 2008		
GOVERNMENTWIDE GRADE 2007: C (2006: C-)					
	2007	2006		2007	2006
DEPARTMENT OF JUSTICE	A+	A-	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	C-	D-
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+*	A+	DEPARTMENT OF STATE	D*	F
ENVIRONMENTAL PROTECTION AGENCY	A+	A-	DEPARTMENT OF EDUCATION	D-	F
NATIONAL SCIENCE FOUNDATION	A+*	A+	DEPARTMENT OF COMMERCE	F	F
SOCIAL SECURITY ADMINISTRATION	A*	A	DEPARTMENT OF TRANSPORTATION	F	B
HOUSING AND URBAN DEVELOPMENT	A	A+	DEPARTMENT OF LABOR	F	B-
OFFICE OF PERSONNEL MANAGEMENT	A-	A+	DEPARTMENT OF DEFENSE	F	F
GENERAL SERVICES ADMINISTRATION	A-	A	DEPARTMENT OF THE INTERIOR	F	F
DEPARTMENT OF ENERGY	B+	C-	DEPARTMENT OF TREASURY	F	F
DEPARTMENT OF HOMELAND SECURITY	B	D	NUCLEAR REGULATORY COMMISSION	F	F
DEPARTMENT OF HEALTH AND HUMAN SERVICES	B	B	DEPARTMENT OF VETERANS AFFAIRS**	F	N/A
SMALL BUSINESS ADMINISTRATION	B-	B+	DEPARTMENT OF AGRICULTURE	F	F

FISMA and DHP-SIRT

FISMA Reporting Roles

- FISMA Reporting is done at the Component level (TMA, DoD, agency, etc.) for systems controlled by that Component
- TMA Privacy Office answers FISMA questions on TMA system's Privacy protections
- TMA Privacy Office provides supporting documentation to verify its FISMA report

FISMA and DHP-SIRT

FISMA Report

- Annual or quarterly report on system security

FISMA and DHP-SIRT

FISMA Report - Privacy

- Privacy section includes:
  - Senior Agency Official for Privacy (SAOP) responsibilities
  - Information regarding privacy and training
  - Privacy Impact Assessment (PIA) and web privacy policies and processes
  - Privacy Act reviews
  - Policy compliance reviews
  - Persistent tracking technology utilization
  - Contact information

FISMA and DHP-SIRT

FISMA Report - Privacy Template

Section D - Senior Agency Official for Privacy (SAOP): Question 1

Agency Name:	**Department of Defense**	**Submission date:**	October 1, 2008

1. Inventory of Systems that Contain Federal Information in Identifiable Form which require a PIA or SORN

In column (a) of the table below, identify by component/bureau the number of agency and contractor information systems that contain Federal information in identifiable form. In column (b), identify the number of agency and contractor systems in (a) for which a Privacy Impact Assessment (PIA) is required under the E-Gov Act. In column (c), identify the number of agency and contractor systems in (b) covered by an existing PIA. In column (d), identify the number of systems in (a) for which a system of records notice (SORN) is required under the Privacy Act. In column (e), identify the number of systems in (d) for which a current SORN has been published in the Federal Register.

Extend the table as necessary to include all components/bureaus.

For the purposes of this inventory, the number of systems covered by an existing PIA cannot exceed the number of systems for which a PIA is required under the E-Government Act, and the number of systems for which a current SORN has been published cannot exceed the number of systems for which a SORN is required under the Privacy Act.

	a.			b.			c.				d.			e.			
	Number of systems that contain Federal information in identifiable form			Number of systems in (a) for which a Privacy Impact Assessment (PIA) is required under the E-Gov Act			Number of systems in (b) covered by an existing PIA				Number of systems in (a) for which a system or records notice (SORN) is required under the Privacy Act			Number of systems in (d) for which a current SORN has been published in the Federal Register			
Component/Bureau	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	% Complete	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	% Complete
Example Component ABC	*100*	*100*	*200*	*75*	*35*	***110***	*75*	*25*	***100***	***91%***	*82*	*69*	***151***	*80*	*68*	***148***	***98%***
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
			0			0			0				0			0	
Agency Totals	100	100	200	75	35	**110**	75	25	**100**	**91%**	82	69	**151**	80	68	**148**	**98%**

FISMA and DHP-SIRT

FISMA Report - Privacy Template

(continued)

2. Links to PIAs and SORNS		
2.a.	Provide the URL of the centrally located page on the agency web site listing working links to agency PIAs: (Hyperlink not required)	
2.b.	Provide the URL of the centrally located page on the agency web site listing working links to the published SORNs: (Hyperlink not required)	
3. Senior Agency Official for Privacy (SAOP) Responsibilities		
3.a.	Can your agency demonstrate through documentation that the privacy official participates in all agency information privacy compliance activities (i.e., privacy policy as well as IT information policy)? Yes or No.	
3.b.	Can your agency demonstrate through documentation that the privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19? Yes or No.	
3.c.	Can your agency demonstrate through documentation that the privacy official participates in assessing the impact of technology on the privacy of personal information? Yes or No.	
4. Information Privacy Training and Awareness		
4.a.	Does your agency have a policy in place to ensure that all personnel (employees, contractors, etc.) with access to Federal data are generally familiar with information privacy laws, regulations and policies, and understand the ramifications of inappropriate access and disclosure? Yes or No.	
4.b.	Does your agency have a program for job-specific and comprehensive information privacy training for all personnel (employees, contractors, etc.) directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities? Yes or No.	
5. PIA and Web Privacy Policies and Processes		
Section 208 of the E-Government Act requires that agencies (a) conduct PIAs under appropriate circumstances, (b) post web privacy policies on their web sites, and (c) ensure machine-readability of web privacy policies. **Does the agency have a written policy or process for each of the following? Indicate Yes or No for each item in the table below.**		
PIA Policies		
a.	Determining whether a PIA is needed	
b.	Conducting a PIA	
c.	Evaluating changes in business process or technology that the PIA indicate as necessary	
d.	Ensuring systems owners and privacy and IT experts participate in conducting the PIA	
e.	Making PIAs available to the public in the required circumstances	
f.	Making PIAs available in other than required circumstances	
Web Policies		
g.	Determining continued compliance with stated web policies	
h.	Requiring machine-readability of public-facing agency web sites (i.e. use of P3P)	

FISMA and DHP-SIRT

FISMA Report - Privacy Template

(continued)

6. Reviews Mandated by Privacy Act of 1974, the E-Government Act of 2002, and the Federal Agency Data Mining Reporting Act of 2007

OMB Circular A-130 (Section 3, Appendix 1) requires agencies to conduct Privacy Act mandated reviews, and to be prepared to report to the Director of OMB on the results of those reviews.

In the table provided, indicate which reviews were conducted in the last year by component/bureau by placing an X in the corresponding cells. For d, e, i, j, k, provide the number of reviews conducted during the last year.

Extend the table as necessary to include all components/bureaus.

	a.	b.	c.	d.	e.	f.	g.	h.	i.	j.	k.	l.
Component/Bureau	Section M Contracts	Records Practices	Routine Uses	Exemptions	Matching Programs	Training	Violations: Civil Action	Violations: Remedial Action	System of Records	(e)(3) Statements	Privacy Impact Assessments and Updates	Data Mining Impact Assessment

FISMA and DHP-SIRT

FISMA Report - Privacy Template

(continued)

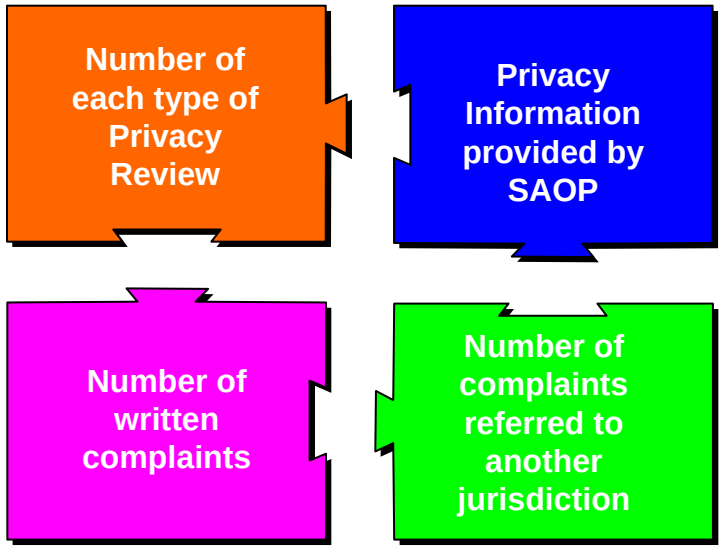
8. Policy Compliance Review		
8.a.	Does the agency have current documentation demonstrating review of compliance with information privacy laws, regulations, and policies? Yes or No.	
8.b.	Can the agency provide documentation of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified in compliance reviews? Yes or No.	
8.c.	Does the agency use technologies that enable continuous auditing of compliance with stated privacy policies and practices? Yes or No.	
8.d.	Does the agency coordinate with the agency's Inspector General on privacy program oversight? Yes or No.	

10. Agency Use of Persistent Tracking Technology		
OMB policy stated in M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002", prohibits agencies from using persistent tracking technology on web sites, except in compelling circumstances as determined by the head of the agency (or designee reporting directly to the agency head).		
Indicate Yes or No for each item in the table below.		
Persistent Tracking		
a.	Does the agency use persistent tracking technology on any web site?	
b.	Does the agency annually review the use of persistent tracking?	
c.	Can the agency demonstate through documentation the continued justification for, and approval to use, the persistent tracking technology?	
d.	Can the agency provide the notice language or citation for the web privacy policy that informs visitors about the persistent tracking?	

FISMA and DHP-SIRT

New FISMA Requirements

- OMB 08-09, “New FISMA Privacy Reporting Requirements for FY 2008” January 18, 2008



FISMA and DHP-SIRT

FISMA Report - New Requirements

7. Written Privacy Complaints

In the table provided, indicate the number of written complaints for each type of privacy issue allegation received by the SAOP, in addition to the number of complaints for each type each type of complaint. Written complaints do not include Freedom of Information Act requests or Privacy Act access requests:

Type	Number of complaints
a. Process and Procedural -- consent, collection, and appropriate notice)	
b. Redress -- non-Privacy Act inquiries seeking resolution of difficulties or concerns about privacy matters	
c. Operational -- inquiries regarding Privacy Act matters not including Privacy Act requests for access/ and/or correction	
d. Referrals – complaints referred to another agency with jurisdiction	

9. Information About Advice Provided by the SAOP

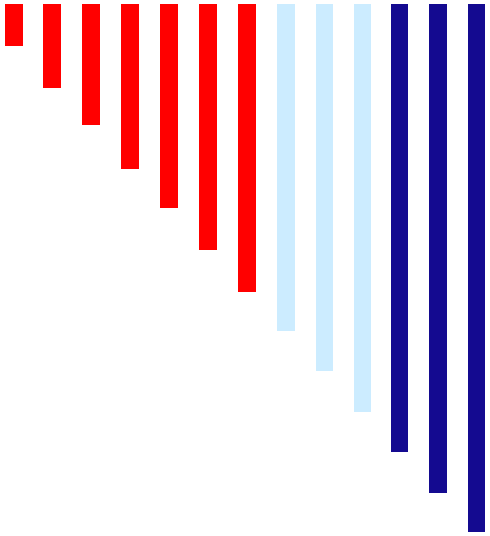
Please state "Yes" or "No" to indicate if the SAOP has provided formal written advice in each of the listed categories, and briefly describe the advice in the space provided. For descriptions of training, please provide the number of employees (or contractors) who participated in the training.

9.a.	Agency policies, orders, directives, or guidance governing agency handling of personally identifiable information	
	briefly describe the advice:	
9.b.	Written Agreements (either Interagency or with Non-Federal Entities)	
	briefly describe the advice:	
9.c.	Reviews or feedback outside of the SORN and PIA process (e.g. formal written advice in the context of a budgetary or programmatic planning)	
	briefly describe the advice:	
9.d.	Privacy Training (either stand-alone or included with training on related issues)	
	briefly describe the advice:	

FISMA and DHP-SIRT

FISMA Report Disposition

- TMA Privacy Office FISMA report forwarded to Defense Privacy Office
- Defense Privacy Office compiles findings from DoD agencies into consolidated FISMA report
- FISMA reports from Federal agencies and departments sent to OMB



DHP-SIRT

FISMA and DHP-SIRT

Reasons for DHP-SIRT

- DoD Information Technology Portfolio Repository (DITPR)
  - Authoritative inventory of DoD systems
  - Allows for consistent compliance reporting across DoD
- OSD Memo, “Defense Health Program Systems Inventory Control Policy” September 16, 2005
  - Required that the Military Health System (MHS) establish inventory

FISMA and DHP-SIRT

DHP-SIRT Information Areas

- DHP-SIRT Inventory Requirements include:
  - FISMA
  - Privacy
  - Business Enterprise Architecture (BEA)
  - E-Authentication
  - Interoperability
  - Enterprise Information Environment Missions Area
  - Standard Financial Information Structure/Federal Financial Management Improvement Act
  - Warfighting Mission Area
  - Enterprise Transition Planning

FISMA and DHP-SIRT

DHP-SIRT Privacy Requirements

- DHP-SIRT Privacy Requirements include:

Privacy Impact Assessment Information	**Privacy Act Information**
Website Privacy Information	**Personally Identifiable Information Determination**

FISMA and DHP-SIRT

New DHP-SIRT Privacy Requirements

- New PIA Requirement:
  - Does the system collect PII from members of the public, federal employees, and/or contractors?
- New SSN Requirements:
  - Are SSNs being used within the system?
  - What is the primary legal legislative or legal justification for SSN use?
  - What is the specific legislative or legal reference for SSN use?
  - Are any Department of Defense (DD) or Secretary of Defense (SD) forms being used that contain SSNs?

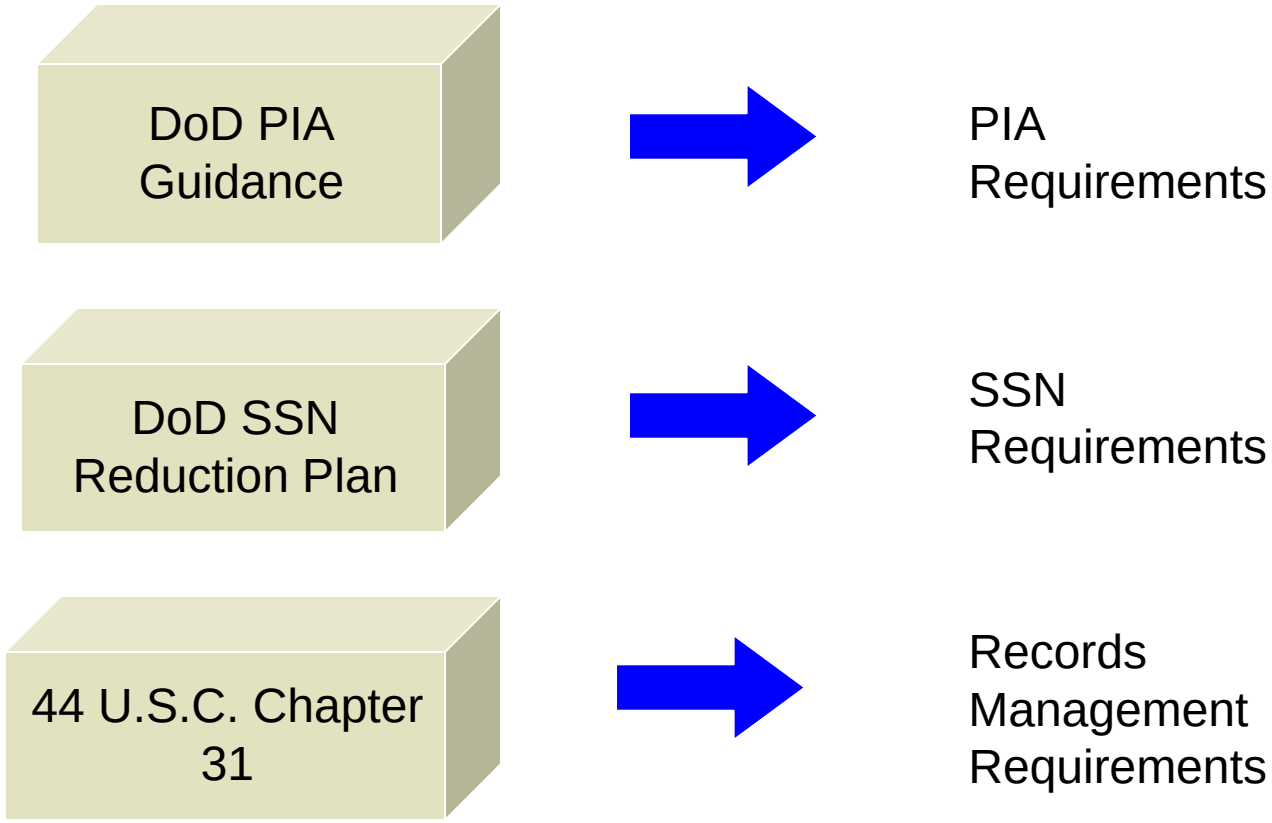
FISMA and DHP-SIRT

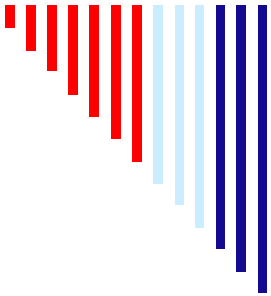
Additional DHP-SIRT Requirements

- New Records Managements Requirements:
  - New Records Management Information Area
    - Does the system contain records data?
    - Has the system been scheduled with National Archives and Records Administration (NARA)?
    - What is the records data disposition authority?
    - If not scheduled with NARA when will it be scheduled?
    - Comments?

FISMA and DHP-SIRT

Reasons for New Requirements





FISMA and DHP-SIRT

Summary

- You now can:
  - Understand the purpose of FISMA
  - Understand Privacy reporting related to FISMA
  - Identify the new Privacy requirements for FISMA
  - Understand DHP-SIRT and its impact
  - Identify the new data fields associated with Privacy in DHP-SIRT